

— v1.1 • iOS

Catpaw

先你一步，把事办妥

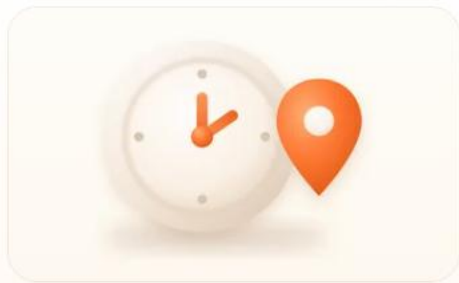
A step ahead. Things handled.

住在 iPhone 里的贴心助理：替你记着、替你盯着，到点主动提醒。



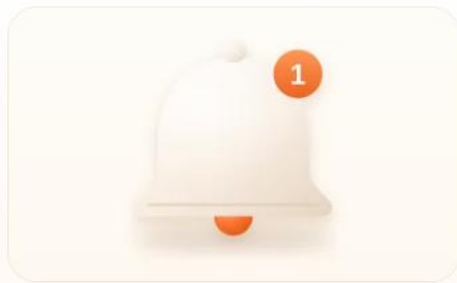
01 问题

要记的事太多，提醒全靠自己



要记的事太多

日程、待办、偏好，都得自己放在心上。



提醒全靠自己

比如开会前 10 分钟，只能自己设闹钟、自己盯着。



AI 只会问一句答一句

你不问它不开口；答完了，事情还得你自己去办。

现在的 AI 助理要等你先开口，答完还得你自己办。
我们想要一个**会先开口、能把事办完、又让人放心**的助理。

01 理念与定位

贴心助理：先你一步，把事办妥

我们的理念

贴心助理：不用自己记、不用自己提醒；安全、简单。

一句话定位

Catpaw，先你一步，把事办妥。

一个住在 iPhone 里的贴心助理，替你记着、替你盯着，到点主动提醒，你点一下就办好。

1

不用自己记，也不用自己提醒

看日历、记偏好，到时候主动来提醒你。

2

把交代的事，变成可用成果

结果直接写进系统的提醒事项和日历，不只是给你建议。

3

安全、简单

进度看得见，动手前先问你；打开就能用，不用注册。

01 一个场景看懂 Catpaw

一个场景：快开会了，它先来找你

1



你说过一句

「我开会喜欢提前 10 分钟到。」它把这句记成你的偏好。

有记忆

2



快开会了，卡片先出现

主动卡片先来找你：按你的偏好提前 10 分钟提醒，并写明「参考了 1 条记忆」。

主动

有记忆

3



点一下「创建提醒」

这一下就是确认。写进系统的提醒事项，成功后给你回执，也能撤销。

可信

能执行

4



到点提醒

10 分钟前，系统提醒事项在锁屏上响起：手机本地发出，不靠服务器推送。

主动

能执行

5



小猫「完成」

小猫的表情就是当前状态：事办完了，它就笑。

看得见

四项要求都在这一个场景里：主动 · 有记忆 · 能执行 · 可信。后面每页都回到这个场景；演示视频拍的也是它。

01 理念 · 同类产品对照

同类产品：借鉴什么，有什么不同

产品	它是什么	我们借鉴	Catpaw 的不同
ChatGPT Pulse OpenAI	每天早上推一份卡片简报	主动卡片，说明为什么	按具体时刻触发，当场办完
Gemini Live Google	语音优先，跨 Google 应用办事	「任务+触发条件」	iOS 原生，执行前先确认
Apple Intelligence Apple	个人上下文，在 App 里执行	深度用好系统能力	会主动找你，记忆可查可删
Now Brief Samsung Galaxy AI	按时间地点生成锁屏卡片	锁屏入口，少打扰	在对话里接着把事办完

只写取舍，不比高下。另有三款通用代理（Grok Bot、Meta Muse、OpenAI dots（ChatGPT））的五项对比，见附录 C。

01 四项能力 · 主动

主动：到点之前，先来找你

场景 · 第 2 步

到点前先来找你，说明为什么，点一下就办好

看你的日程：10:23 有个产品评审会，卡片先出现，问你要不要 10:13 提醒，并写明「参考了 1 条记忆」。

信号	状态	用来做什么
时间	已交付	到点前，按你的提前量来提醒
日程	已交付	看日历里的下一个会
位置	部分	只用在附近查询和出发提醒，只在使用 App 期间
消息	v1.2 计划	读 Gmail 发现会议和航班（只读）

打扰有分寸

你会 怕助理太吵，最后只好关掉它。

它会 不急的事只在 App 里放一张卡，要紧的才响铃；晚上 22 点到早上 8 点不响；手机上每天最多响 5 次，再多只放卡片、不响铃。

好处 每张卡都告诉你为什么出现，也能一键撤销。



实拍：「主动」列表里的主动提醒卡

部分 服务端推送还没配置：现在到点提醒都由手机本地发出。

02 四项能力 · 有记忆

有记忆：记住你的偏好，并且真的用上

场景 · 第 1-2 步

你说过一次，它就记住，并按你的习惯来

你说过「我开会喜欢提前 10 分钟到」（需开启自动记住），之后的提醒按 10 分钟来；卡片写着「参考了 1 条记忆」，点一下就能看、改或忘记。

会记什么，不记什么

你会 不想每次都重复交代，又怕它乱记。

它会 只记稳定的偏好、身边的人和常用事实；不记密码、健康和财务信息。

好处 该记的记得住，敏感的不碰。

你说了算

你会 它记错了，或者你不想让它记。

它会 设置里有总开关，可以更正，也可以「忘记」。

好处 忘记之后，不会从旧对话里再学回来。



实拍：设置 > 记忆，偏好「我开会喜欢提前 10 分钟到」

实拍：「本次用到的记忆」面板，可编辑、可忘记

v1.2 计划 长对话自动摘要、按意思检索记忆（现在按关键词）。

03 四项能力 · 能执行

能执行：手机本地能力 + 系统 App

场景 · 第 3-4 步

确认后再做：写进你的日历和提醒事项

先出确认卡，点「加入」或「创建提醒」才写进系统日历或提醒事项，提醒到点在锁屏响起（本地）；写成功才给回执，没权限会告诉你怎么开。

有地点的会，算上路程

- 你会** 要赶去别处开会，怕路上来不及。
- 它会** 会议有地点时，还会算上路程；快来不及时，锁屏和灵动岛出现「该出发了」倒计时。
- 好处** 不用自己算几点出门。

v1.2 计划 生成图片、按任务选模型、读 Gmail。

读网页，写报告

- 你会** 想让它查资料，再给你结论。
- 它会** 读你给的公开网页链接，写成带出处的报告；信息不够会先问你。
- 好处** 结论能追到原文。



实拍：加入日历前先出确认卡（加入 / 编辑 / 取消），并标出本次用到的记忆

04 四项能力 · 可信

可信：先问你，再动手；说实话

场景 · 第 3 步

动手前一定先问你；做没做成，按系统回执说实话

点「加入」或「创建提醒」这一下就是确认；系统给了回执才说「已加入」，还能撤销。

为什么

主动卡片说明为什么出现；状态只显示真实发生的步骤。

看到什么

图片先征得你同意，换了处理图片的模型会重新问你；位置只在使用 App 期间；日历按系统授权。

记住什么

记忆有总开关，可以更正、可以忘记。

做什么

点了确认才执行；结果不确定就写「未确认」；做完能撤销。



实拍：日历回执「已加入日历」，可撤销

03 交互亮点 ① 看得见

看得见：不用守着屏幕，也知道办到哪了

进度到处看得见

代码已实现

聊天里有状态行；锁屏和灵动岛有实时活动。

锁屏时会按隐私设置隐藏标题。

为什么 不用一直盯着 App，也知道它在干什么。

边生成边看

代码已实现

回复一边生成一边显示，还有等待时的光效。

为什么 不用干等一整段回复。

毛绒小猫陪你

代码已实现

6 个状态：等待、思考、写回复、执行、完成、出错。

为什么 它的表情就是当前状态，一眼就懂，不用看文字。



示意：锁屏实时活动（按 593 代码画，非实拍；标题为演示文字）

03 交互亮点 ② 不跳页

不跳页：要你决定的事，就在对话里办完

确认卡就在消息里

已交付

需要你拍板时，卡片直接出现在这条消息下面。

为什么 人不用离开对话，也不会漏掉。

示意图（非截图）· 场景第 2 步的卡片

10:30 周会 · 要我 10:20 提醒你吗？

参考了 1 条记忆

创建提醒

稍后

不用了

生成式 UI

已交付

它直接给你一张能填的表：日期、时间、数字、开关、选择。

为什么 不用一问一答来回好几轮。

示意图（非截图）· 订一个会

日期

选择日期

时间

选择时间

人数

— +

提前提醒

开 / 关

提交

语音

已交付

听写：按住说话，或点一下进入全屏听写。

为什么 手上不方便打字时，说就行。

真机修复中

完整语音对话（说 → 回 → 读）：真机还在修，这次不演示。

03 设计 · 为什么这样做

设计：每个选择都为“从容，清楚，可靠”



品牌板（用户提供）

品牌

logo 是猫耳和猫爪，加一道向前的笔触，就是「先你一步」。暖橙代表温暖、值得托付。

看得清

亮橙只用在图形上，文字用对比度够高的深色；字体跟随系统，调大字号的人也看得清。

一致

不弹浮层，状态就在消息上；全 App 只有一个输入框；小猫的每个动作都对应真实状态。所以你不用学。

方便

打开就能用，不用注册，以后再绑定 Google，数据不丢；也可以用 Siri 或快捷指令一句话打开。

04 安全与账号

安全与账号：你的数据，只归你

每个人只能看到自己的数据；密钥不进 App

你的记忆、图片和账号，都按「只归你、可以删、退出就清掉登录凭证」来设计。

你的数据只归你

- 每个人只能读到自己的数据。
- 密钥只放在服务器上，App 和代码里都没有。
- 每次请求都校验你是谁。

你的记忆和图片

- 记忆可以更正，也可以忘记。
- 图片用完即删，之后只留文字。
- 记忆只当参考资料，不当指令执行，防止被注入。

你的账号

- 体验账号直接开始，以后升级不换号。
- 退出登录时，就算没网，也会清掉手机上的登录凭证。



实拍：账户菜单（体验账号、使用 Google / GitHub 继续、退出登录）

04 技术 ① 选型

选型：站在开源肩膀上，把「原生 + 可信」留给自己

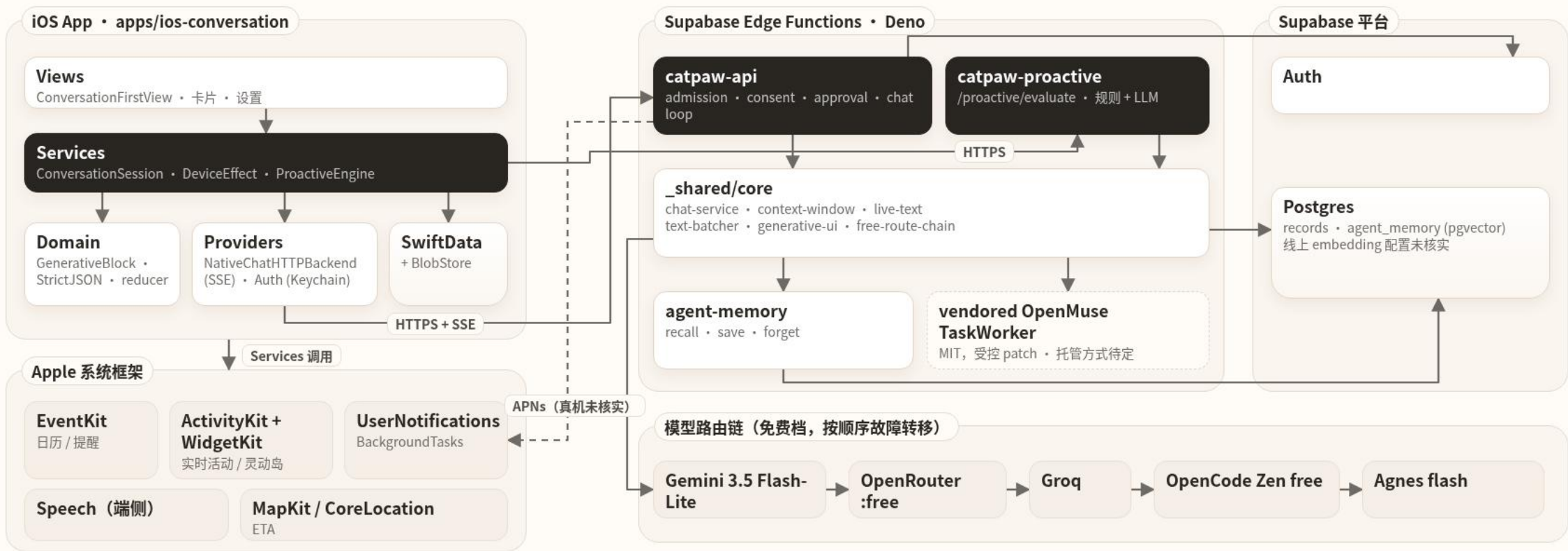
按固定 commit 源码核读 4 个 CopilotKit 系开源项目和 SDK（只读源码，没有安装运行、没有接真实模型）：没有一个能直接当 SwiftUI App 的底座。

看过什么	关键发现	决定	不采用 / 原因
OpenMuse @1ac68f39	RN 客户端；TaskWorker 的 lease / checkpoint；审批绑定参数 hash、结果未知不重放	复用 TaskWorker（MIT 受控 vendoring） 借鉴 审批 hash、结果未知语义	不 fork RN 客户端：保持 SwiftUI 原生；worker 托管方式仍 待定 (Proposed)
CopilotKit / OpenDots @625452e0	React Web；按工具授权、可重新打开的审批卡、revision 防覆盖	借鉴 审批卡语义	不迁移：依赖 Intelligence、SQLite，单 owner 设计
OpenBot	consume / result / continuation；强依赖 Intelligence	借鉴 续跑语义	不接入完整 Bun / Intelligence 运行时
OpenIntelligentUI @9c982df1	受控组件 registry、A2UI catalog、HTML 沙箱	借鉴 registry + schema 自建 Swift typed registry	不采用任意 HTML 沙箱和整套 Next / Python 栈
CopilotKit SDK / AG-UI @7e97c05d	事件语义好，但没有 Swift SDK	借鉴 事件分层 自建 SSE 契约 catpaw.native-chat.v1	—
Supabase	Auth、Postgres、Edge、pgvector	复用 整体	—
Apple 框架	EventKit、ActivityKit、Speech、MapKit、BGTasks	复用 整体	不自己做推送和日历同步
免费模型供应商 × 5	免费额度易 429	复用 OpenAI 兼容接口、Gemini Interactions 自建 路由链、故障转移、同意绑定	—

复用 直接用 **借鉴** 学语义、自己实现 **自建** 自研。CopilotKit Intelligence 托管服务未使用。

04 技术 ② 系统全景

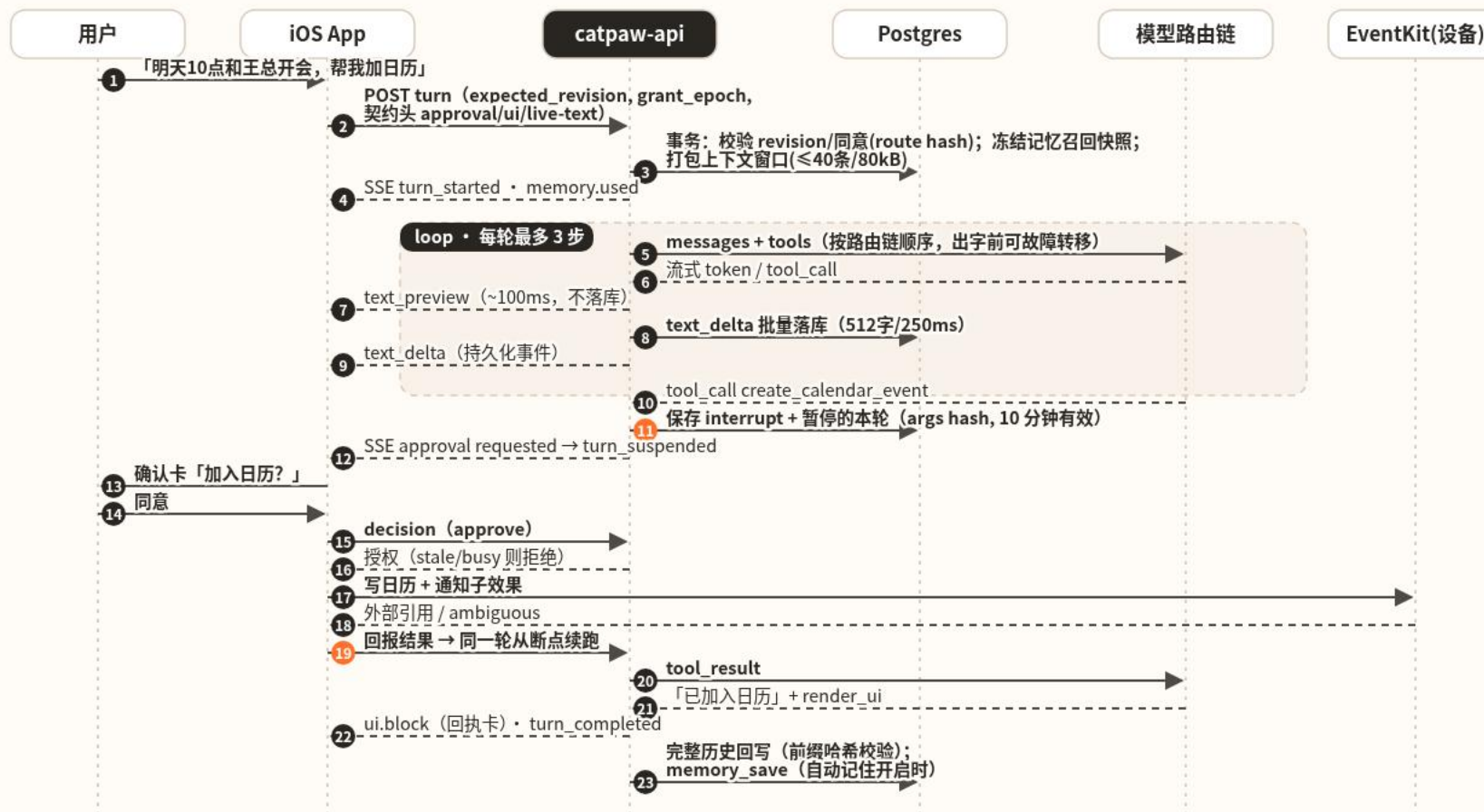
系统全景：原生 App、两个 Edge 函数、Postgres



iOS 五层：授权在后端，View 不发 HTTP、不执行副作用。线上 catpaw-api v53；记忆表 pgvector，向量检索的线上 embedding 配置未核实，无向量时退回词法。

04 技术 ③ Agent 怎么跑

一轮：准入 → 模型 ⇌ 工具 → 人确认 → 设备执行 → 续跑



准入在一个事务里

校验 revision / grant, 冻结记忆快照, 打包上下文窗口; 请求体上限 40 kB。

每轮最多 3 个模型步

工具结果回灌后继续; 每一步先写 dispatch checkpoint。

工具按风险分级

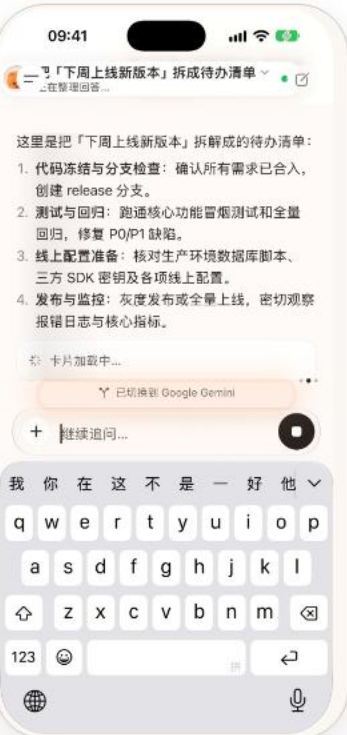
只读 / 可撤销直接跑; 日历、提醒、外部写每次都要确认; 创建待办首次确认; 未声明的工具默认最严。

暂停与续跑是同一轮

审批时把本轮存为 checkpoint (⑪), 批准后从断点继续 (⑲ 起)。

04 技术 ④ 交互三件套

流式实时预览 × 生成式 UI × 人在回路



流式实时预览

已上线

两条通道：持久事件
`text_delta` 512 字 / 250 ms 批量落库，断线按 turn + sequence 续传。

预览 `text_preview` 约 100 ms 一帧，不入库；需请求头 `X-Catpaw-Live-Text: 1`。

坏帧丢弃；失败或取消时以持久事件为准。

实拍：回复已出、卡片还在加载；提示「已切换到 Google Gemini」



生成式 UI

已上线

受控 registry，不让模型写代码：9 类 block (card、choices、confirm、form、sheet、list、progress、place、event)。

服务端校验字段与上限 (actions ≤ 3、字段 ≤ 8、payload ≤ 32 KB)。

地点 / 日程卡内容由服务端从工具结果填充，模型不能编。

实拍：加入日历确认卡



人在回路

已上线

审批绑定
`argsHash(name+arguments)`，10 分钟有效：同意 / 拒绝 / 以后同类直接执行。

授权在后端，设备只执行并回报；结果未知只核对、不自动重发。

需要回应的卡片和审批走同一套中断机制。

实拍：日历回执「已加入日历 · 撤销」

04 技术 ⑤ 主动与记忆

会「找你」，也说得清「为什么找你」



04 技术 ⑥ 可靠性

免费模型也能稳：不重发、不丢历史、可恢复



05 状态与路线

v1.1 做到了哪里，v1.2 要做什么

已交付 v1.1

- 看日程主动提醒，说明为什么，可撤销
- 记住偏好并用在提醒上；可更正、可忘记
- 写进提醒事项和日历，有回执
- 锁屏、灵动岛、桌面小组件
- 状态行、实时文字、小猫、可填表单、听写
- 动手前确认；图片先征得同意

部分 还差一步

位置 部分

只用在附近查询和出发提醒

提醒送达 部分

服务端推送还没配置，现在靠手机本地通知

语音对话 真机修复中

真机修复中，这次不演示

v1.2 计划 计划

更主动

读 Gmail 发现会议和航班；配好服务端推送

更懂你

长对话自动摘要；按意思检索记忆

更能干

生成图片；按任务选模型；语音对话完善（回声消除、逐句朗读）

都还没有发布，也没有日期。



先你一步， 把事办妥

A step ahead. Things handled.

不用自己记，不用自己提醒；安全，简单。



版本在哪，哪些还不能对外承诺

生产（服务端）
catpaw-api v53 (59b5aae6, 10-17 22:21 上线);
catpaw-proactive v9。

当前安装（iOS）
1.1.0 (build 593), chore/v11-release 80c7c166: 已原地装到模拟器和 iPhone 13 (release/mac-logs/head-2ec9e3e6/REPORT.md 09:08)。

1.1.0 终版状态
含 3 个真机问题的修复提交；CHANGELOG 仍标「未发布」、没打 tag；语音对话仍是「真机修复中」。

缺口	现状	下一步
服务端推送	APNs 未配置 (/health apns:false)；到点提醒靠本地通知；视频里的推送标「模拟器推送」	补齐 APNS_* 密钥，不用重新部署
Gemini 条款	条款限制消费者使用、年龄和地区，免费层内容可能被用于改进产品	需要用户决定
真机问题（3 个）	设置按钮没反应；语音对话按钮置灰；语音对话里说话没有回应	1.1.0 终版修复；修好前不演示语音
免费额度	OpenRouter 免费路由 20 次/分钟、50 次/天（余额不足 10 美元），文本和看图共用一个 key	—
模型调用每日上限	未开启	按用户偏好保持不限
模型选择器白名单	清单未核实	—
消息信号	没有实现	v1.2: Gmail 只读
上架与工程	没有 Apple 登录；没有服务端删除会话接口；GitHub Actions 暂无运行机；迁移版本号与生产对不上	计划中

已在 build 41 修复、等终版最终验证：发送后一直转圈、登录后卡在启动页。

一天里的 8 次上线

13:36	9 条迁移, 启用 pg_cron / pg_net	tick 每分钟 200
13:44	catpaw-proactive → v9 (792587e)	/health apns:false
17:01	记忆迁移: grant usage on schema extensions	42501 修复
18:15	catpaw-api → v50: 只读工具不暂停、上下文修复	PR #93
19:20	catpaw-api → v51: 账号级同意	PR #94
19:51	catpaw-api → v52: 看图备用链	PR #95
22:21	catpaw-api → v53 (59b5aae6): 上下文滑动窗口、实时文字	冒烟未批准
22:25	PR #96 合入 main (694d19ec)	= 生产 v53

它们替你跑长任务，我们只把手机上的小事办妥

产品	主动	有记忆	能执行	可信	交互
Catpaw iOS · 只盯手机上的提醒和日程	看日历的下一个会，到点前出卡片和本地通知；22-8 点不响，每天最多响 5 次	长期记忆会改提醒提前量，卡片写明「参考了 N 条记忆」	确认后写进系统提醒事项和日历，给回执	动手前必确认；「为什么找你」和撤销；记忆可更正、可忘记；状态如实	听写；小猫 6 种状态；实时文字；可填表单卡片；锁屏 / 灵动岛实时活动
Grok Bot xAI · 桌面+iOS · 常驻的 AI 同事	常驻，持续工作，需要批准时才回来找你	记住对话，学习做事方式；看一遍就学成例行任务	每个 Bot 有云端电脑：浏览器和终端，能登录你的应用	需要批准时回来；其他权限 / 隐私控制： 未核实	短信式消息线程，手机和桌面接续；多个 Bot 可进群聊
Meta Muse Meta · App、网页、WhatsApp · 仅美国 18+	关掉 App 也继续工作，有变化或需批准时回来；主动给建议	记住之前的对话，可以让它「忘记」	发邮件、订行程、填表、下单（一次性卡）	Secure VM+Sentinel 管上网和许可；碰不到密码和支付信息；可关闭训练使用；不进广告系统	像聊天一样说话；可爱吉祥物；已宣布 Muse Charm 硬件
OpenAI dots (ChatGPT) OpenAI · ChatGPT、Slack、Teams	没人用时做主动研究（只用只读工具），有结果或要你决定时来找你	用过去的对话和你的偏好	云端电脑和浏览器：研究、分析、写文档，可交给 Codex 写代码	Custom Rules：允许 / 需批准 / 禁止；敏感动作先自动审查；Activity View	可以起名、自定义外观

借鉴 Grok Bot
只在需要你拍板时才回来
→ 确认卡

借鉴 Meta Muse
可爱的陪伴形象；可以让它忘记
→ 小猫、记忆「忘记」

借鉴 OpenAI dots
后台主动只读；动手前按规则确认
→ 「为什么找你」、确认卡

借鉴 Pulse / Gemini / Apple
主动卡片；任务+触发条件；系统能力
→ 见第 5 页

老实说：Grok Bot、Muse 和 dots 用云端电脑替你做跨应用的长任务，范围远超 Catpaw。Catpaw 刻意做窄，只盯手机上「到点该提醒你」的事，用 iOS 原生的日历、提醒、锁屏和灵动岛办完，不替你操作网页或付款。只写取舍，不比高下。

每个说法都有出处

编号	出处
E1	ProactiveEngine / WhySheet / Undo / Rules
E2	throttle.mjs+push_throttle 迁移
E3	proactive_tasks / proactive_cron 迁移
E4	NearbyPlaces.swift
E5	agent-memory/contract.mjs
E6	agent-memory/service.mjs
E7	ConversationMemoryView+tombstones
E8	PLAN §1、chat-service.mjs
E9	DeviceCalls、ReceiptCard 等
E10	CatpawWorkLiveActivity.swift
E11	CatpawApp.swift:267-276
E12	core/src/tools.mjs
E13	inline-status、REVIEW-v3 §1
E14	consent.mjs:4-6、image-consent.mjs
E15	ComposerDictation、voice-audit
E16	CatpawPlushMascot.swift
E17	pr-triage/required.yaml
E18	live-text.mjs+测试
E19	GenerativeBlocks/*
E20	brand-theme.md、BrandTokens

编号	出处
E21	NativeAuthSessionManager:183
E22	agent_memory 迁移 (auth.uid())
E23	oss-audit/REPORT.md
E24	authority.mjs:137-153
E25	NativeAuthSessionManager:74-86
E26	free-route-chain、vision-route-chain
E27	对标 Grok Bot: x.ai 发布与扩容公告
E28	对标 Meta Muse: TechCrunch、Gadgets360、AP、Verge
E29	对标 OpenAI dots: The Decoder、文档快照、Agent Log
E30	research/README.md:139-144、assessment-2026-10-13 (源码核读)
E31	adr-005-runtime-reuse、THIRD_PARTY_NOTICES、runtime.mjs:2
E32	docs/architecture.md:25-83
E33	core/src/approval.mjs:1-27
E34	core/src/text-batcher.mjs:1-3、63
E35	core/src/generative-ui.mjs:2-32
E36	proactive/decision.mjs、decision-model.mjs:4-7
E37	core/src/context-window.mjs:1-24、99-120
E38	demo-blockers/DIAG.md (v10 / v54 待部署)
E39	opendots / openbot / openintelligentui-code-review